DOSarrest Security Services
User Guide

Public version 1.5

Table of Contents

Introduction

DOSarrest Security Services (DSS) has been designed as a tool for you to access information about an attack against your sites, as well as manage your account settings. Once logged in, you will be presented with the Dashboard view which gives you statistics based off of the last hour worth of traffic.

Due to the massive amount of information involved, long term statistics are currently not available in the DSS. All statistics displayed will be based upon the last hour's worth of gathered data. Historical data is being logged and will be available in the future.
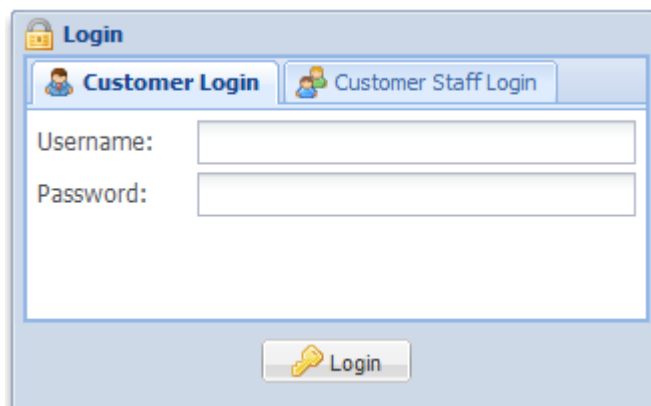
Our DSS provides you with the ability to see connection statistics as well as bandwidth statistics. The connection statistics are based upon a sampling of all open connections every minute. The bandwidth statistics are based off of all TCP traffic associated with the VIP/Origin IP at a proxy level. This includes all health checks and other traffic related to testing functionality of the site.

Our DSS also provides the ability to see how many networks are currently online and the status of connectivity to your servers. You can also access our knowledgebase, access our support system, manage settings for your site, and even manage staff members that can access the DSS.
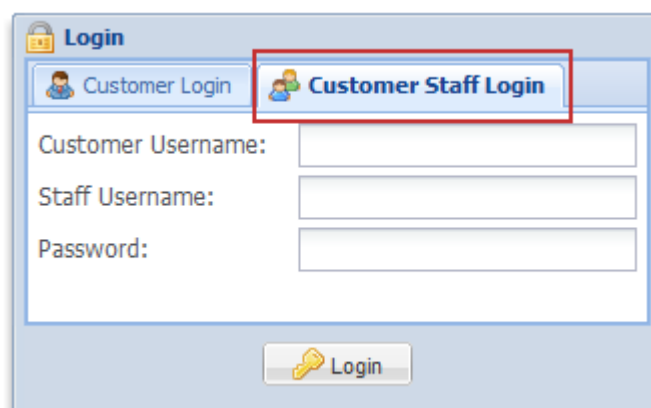
Many more features are planned for the future.

Logging In

To log into DOSarrest Security Services, click on "Customer Login" at DOSarrest.com. When accessing the site for the first time, you will be presented with a login prompt.

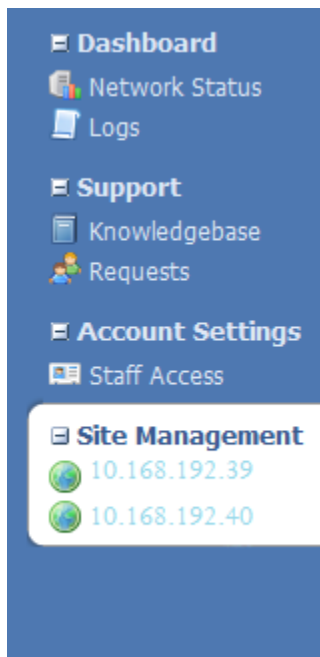Staff members will be able to log in by clicking the "Customer Staff Login" tab and providing the login details.

More information on staff can be found in the Staff Access section.

Navigation

Navigation on the site is controlled by the menu on the left hand side. Tooltips throughout the site will also provide information on many options.


The navigation for the site is currently split into four sections. Each section and its subsections can be accessed. For example, clicking on "Support" will display information about how to get support, and clicking on "Knowledgebase" will display the knowledgebase.

Dashboard

The Dashboard provides quick access to live statistics related to your site. All of the graphs in the dashboard are updated every minute with the latest information.
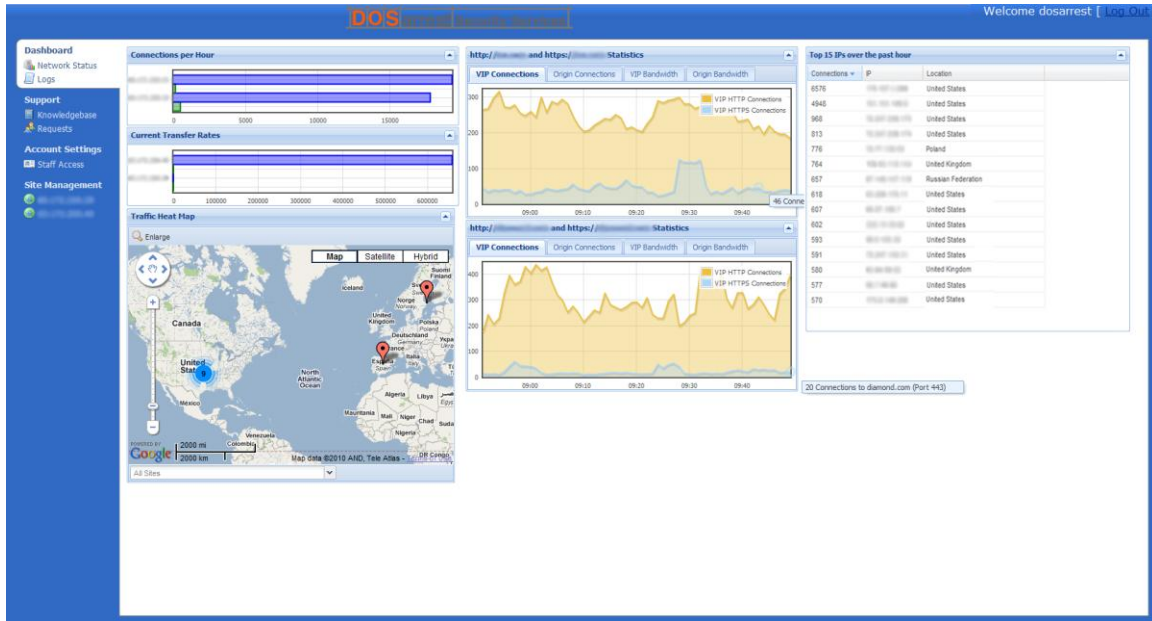

The "Connections per Hour" graph displays an overview of the connections made to your VIP/Origin IP. When hovering over each bar, a tooltip displaying the exact number of connections will appear.
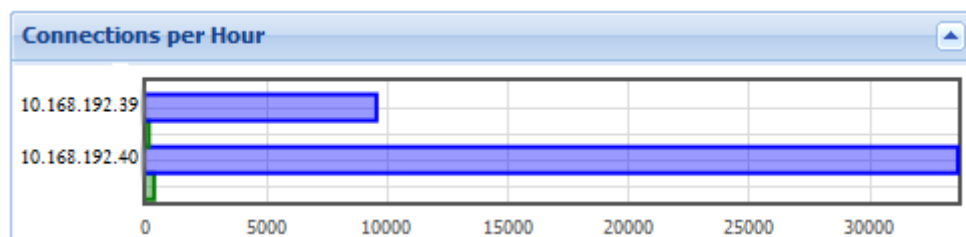

The "Current Transfer Rates" graph displays an overview of the bandwidth to your VIP/Origin IP. You can also hover over each bar here to show the exact transfer rate in Mb/sec.

Current Transfer Rates

10.168.192.39

10.168.192.40

0   1000000   2000000   3000000
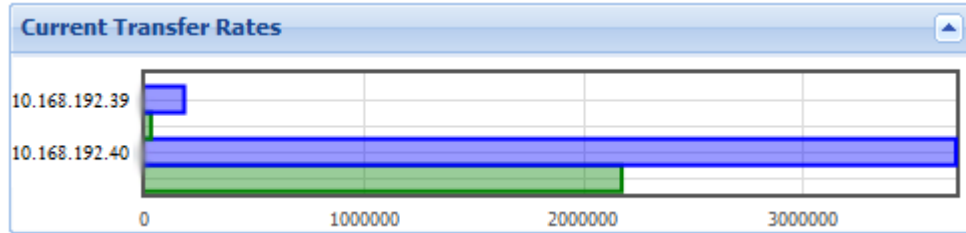
Below the transfer rates is a Traffic Heat Map, which shows which countries the traffic is coming from, and how much of it. It is also color coded, with high numbers shown in large red circles.
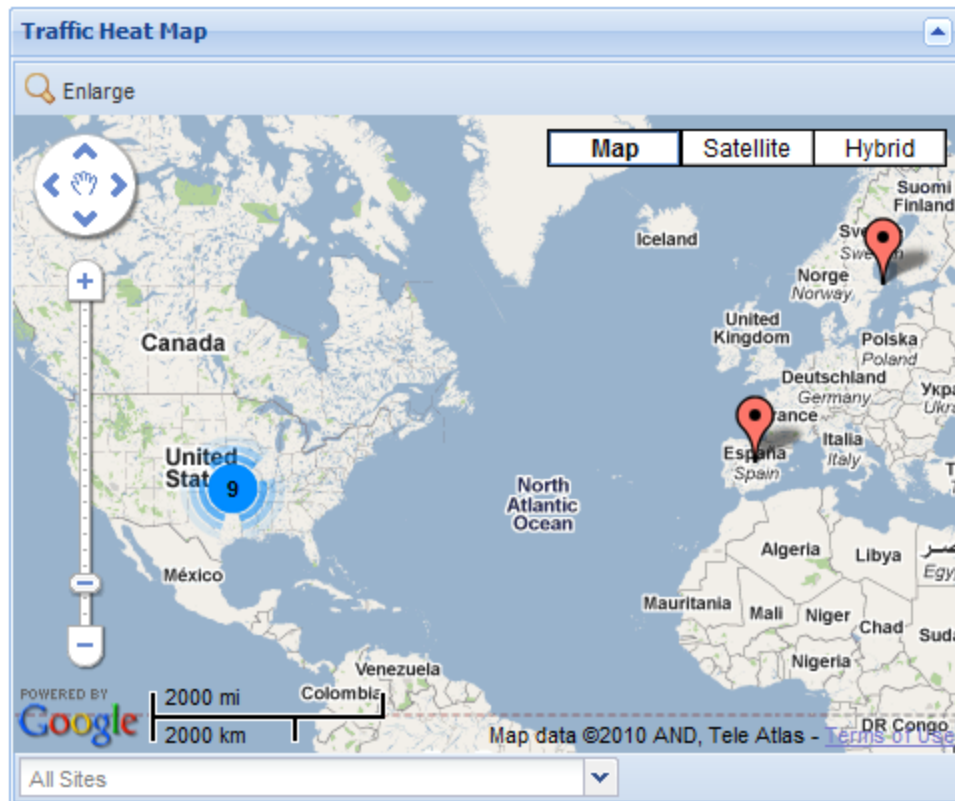
For each every VIP you have, a Portlet will appear in the center column of the Dashboard providing a more detailed breakdown of the two graphs above. The Portlet for each VIP displays four tabs which each contain graphs. The four graphs display the minute by minute data over the past hour obtained from statistics gathering.
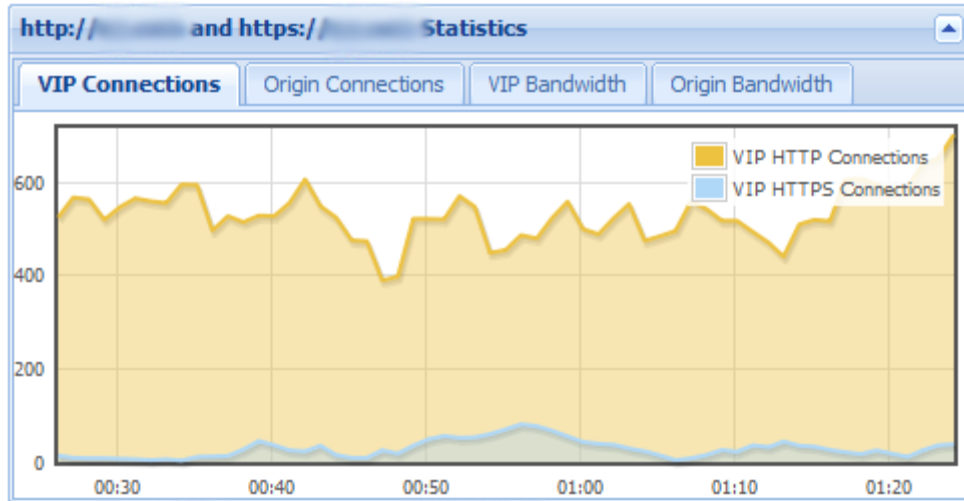
The "Top 15 IPs over the past hour" Portlet provides a list of the top fifteen IPs that logged the most number of connections to your VIPs.

Network Status

The Network Status section shows a list of all online networks in each active geographical region and whether those networks can connect to your origin servers.
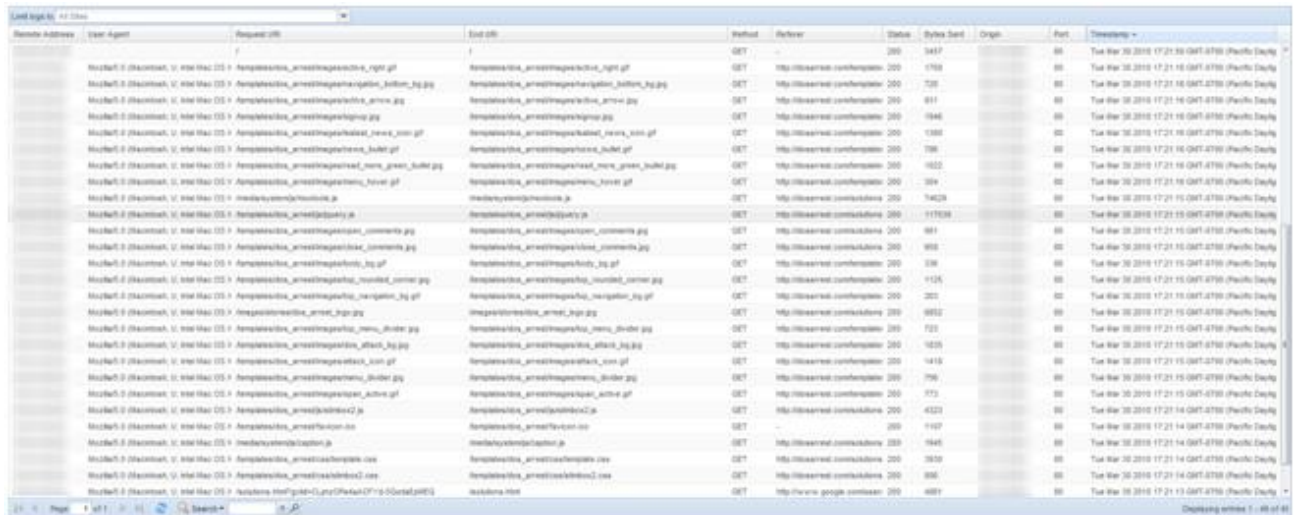

Under the "Status" column, one of three icons will show up. If all servers and connections are stable, a green checkmark will appear. If there are some connectivity problems but the servers can still communicate with your server, a yellow exclamation mark will appear. If none of the servers on a network can communicate with your server, then a red exclamation mark will appear.

Logs

The logs section provides the ability to view the access log entries over the past hour. The logs section shows the typical basic access logs used by web servers. All of the information is separated into customizable columns.

Within our access logs, one additional column has been added which is not in most web server logs. The two columns labeled "Request URI" and "End URI" should be identical unless a visitor has hit our final stage security authentication systems.

At the top, there is a dropdown field, which lists each of your sites. By default this box is set to "All Sites" which displays the log entries for all of your sites. Upon selecting a specific site from the list, the logs will be reloaded and will display only the logs for the site you have selected.

Access logs are only provided upon special request due to the massive amount of data involved during attacks. When a site is under attack, a massive amount of access logs are generated in a very short period of time. This massive amount of access logs requires much processing power in order to provide live access to the logs, so we currently only use it in special cases when it is required.

Support

Clicking on Support from the left menu will display the following:

DOSarrest provides 24/7 support via the following methods:

Online support system:	Request Emergency Help
	View Current Requests
Emergency live chat:	DOSarrest Click here for Live Support
Emergency contact line:	1-888-818-1344

The best way to get effective support with proper history tracking is to use the online support system. If you require assistance, if you would like additional information, or if you would just like to suggest a feature, our online support system will help facilitate your needs. The online support system will also send email notifications to you when a support agent responds. If there is an emergency and you need to contact DOSarrest support right away, we also provide live chat and a toll free number to get in contact with one of our experienced support agents.

Knowledgebase

The knowledge base is split into two areas. The left side allows you to select a specific category of knowledgebase articles to view. By default, the "All Categories" menu item is selected, which will display a list of all knowledgebase articles in the system. Selecting a category from the left menu will limit the articles displayed on the side to just articles in the selected category.
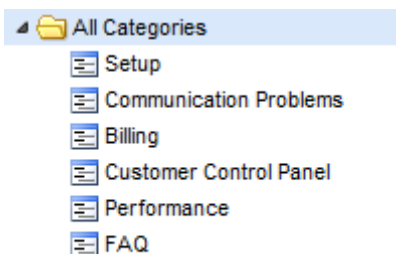
On the right side, knowledgebase articles will be displayed listing the KBID (Knowledgebase ID) and the title. To view the article, simply click anywhere on the row for the article you want to view and a popup will appear.

Using "Pagination", 25 articles are displayed at a time with a menu down at the bottom left allowing navigation between the pages. There is also a search prompt at the bottom which allows you to search the knowledge base for exactly what you are looking for. Simply type something in the search box, and click the magnifying glass. You can clear your search by clicking the X.

Requests
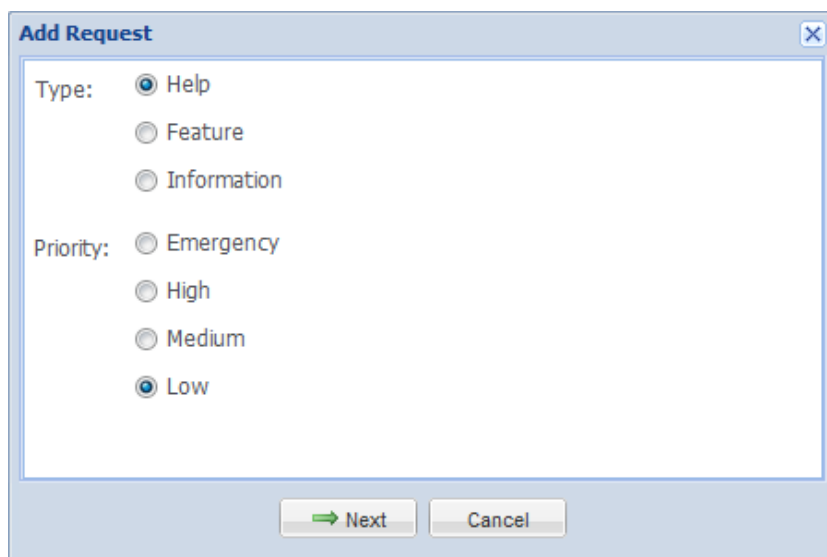
The support requests section has two tabs at the top which display either Active or Resolved support requests. Our support system works on a very basic principle. When you want or need services from us you are "requesting" something. If you need help or information, you are requesting us to do something. So, with our support system, you make "Requests" which we then work on completing. Support requests can only be marked as completed by a support technician who has completed the support requests and received permission from you to mark the request as completed.
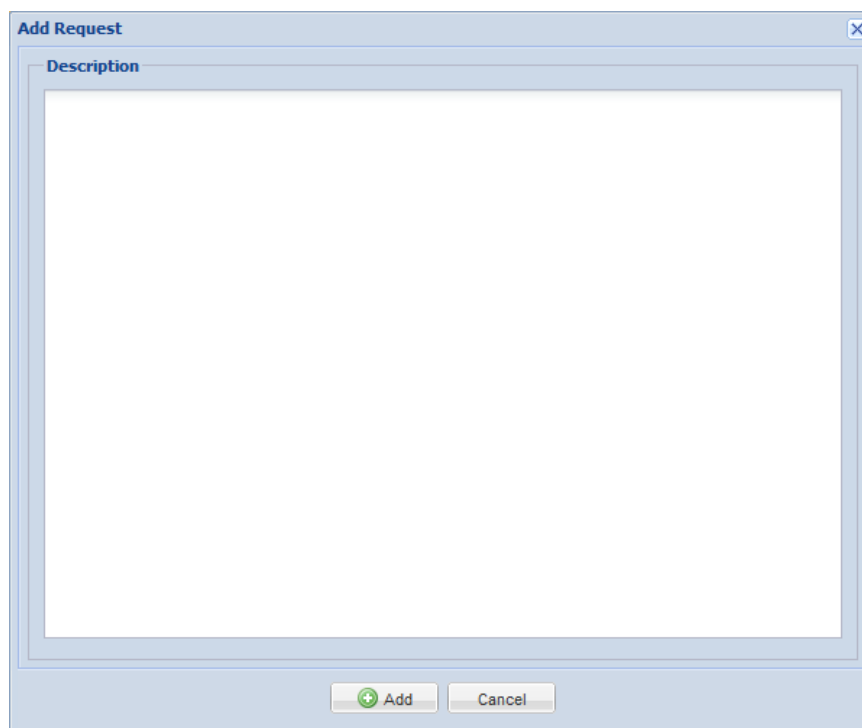
Just like the Knowledgebase, the same pagination and search features are provided at the bottom. To add a request, click the following button located at the top left:
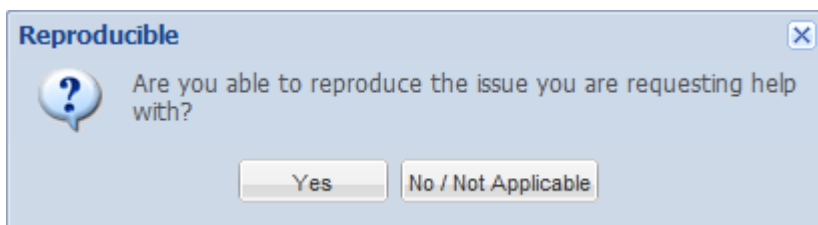
Upon clicking the button, the following popup will appear:

Choose the type of request you are making and how high of a priority you believe it to be. Once you have chosen the appropriate options, click "Next" to continue. If you chose to request Information or a Feature you will be given the following popup window to give a description of what you are requesting.

If you chose to request help, you will see an additional step asking if the issue you are requesting help about is reproducible.

If you clicked "Yes" you will see the following popup. Otherwise, you will see the same popup as when requesting Information or a Feature.

Fill out your request with as much detail as possible.

Once a request has been added, it will immediately show up in the Active Requests table. To open/edit a request, simply left click on the row anywhere to open a popup viewing the request. The popup window will look like the following unless it is an Information/Feature request, in which case the "Description" box would be bigger, and the "Reproducible" section would not appear.
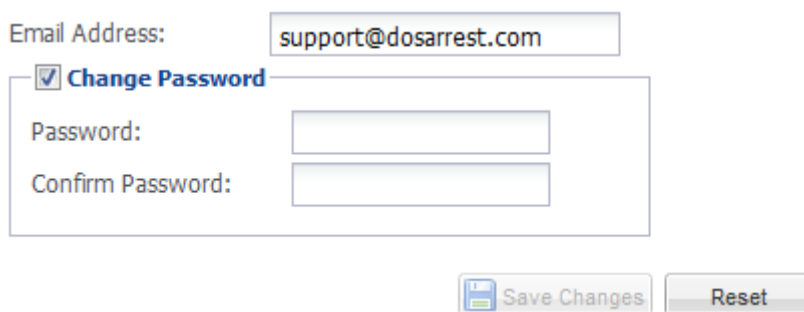
The popup initially shows the Properties tab which displays the basic information regarding the request. The second tab "Communications" allows you to communicate to the Support Agents at any time. The Communications tab is similar to a chat client; once you have opened it, it will update itself with any new posts that Support Agents send. You can control this functionality by toggling the red stop symbol. At the bottom of the Communications tab you can send a message to the Support Staff.

Account Settings

The Account Settings provides you with the ability to change your email address and password.

Simply make your desired changes and click "Save Changes". Clicking reset will reset the form to how it was before you made changes.

Staff Access

Currently staff members who are added have access to everything that you do, except the ability to manage staff members. More control over permissions is planned for the future.

To add a new staff member click the "Add" button at the top left; this will open up a popup with a form to fill out.

Enter the desired Username/Password and an email address, and then click "Add Staff Member". Once the staff member has been added, they will show up in the Staff Access table right away and will be able to log in right away.

To change the password for a staff member, simply click the key icon in the "Actions" column and enter a new password.

To delete a staff member, simply click the red minus sign icon in the "Actions" column.

Once a staff member has been added, to change their username or email, simply click on their username or email, make the changes, and click "Save Changes" up at the top right to apply the changes.

Site Management

Clicking on the "Site Management" section from the left menu provides a form which allows you to request a new site to be added to your account. To request a new site simply enable the protocols (HTTP/HTTPS) which your site uses, and provide the server IP and domain name for the site. You may also specify if you would like Caching on or off for the new site. If you have enabled HTTPS you will also need to provide the SSL Cert/Key used.

Caching is a system we offer to increase the performance on your site and decrease load on your server. It allows us, in short, to copy your entire site onto our servers. This way, content is served much faster as there is not as much communication back and forth from our servers to yours. The default setting for our servers to update the cache of your website is once per hour, but this can be modified in the individual site's settings.
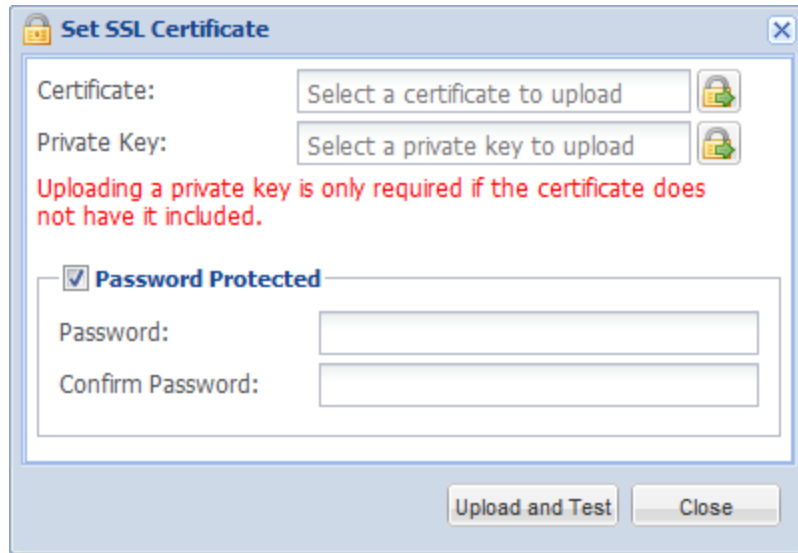
Our system requires the SSL certificate and key to be supplied in order for HTTPS to work. For our servers to be able to use your SSL certificates, they must be in a PEM format. If you already have your certificate and key in PEM format, you can just copy and paste the cert and key into the supplied text boxes. If you have an intermediate cert you can also copy and paste it into the "My SSL Cert" text area under your SSL certificate.

If you have the SSL certificate in some other format, or you would just like to test the certificate, you can click the "Upload SSL Certificate" button which will open up our SSL certificate utility.

Our SSL certificate utility handles converting the certificate to the PEM format we require and testing the certificate to see if it is valid. When uploading a certificate, it can be in any valid format which OpenSSL recognizes such as PEM/CRT/CERT/P12/PFX. If your SSL private key is not included in the uploaded certificate you will have to upload it along with the certificate.

If the certificate you are uploading is password protected provide the password by checking the "Password Protected" option.

Once you have filled out the form correctly, click the "Upload and Test" button to begin the upload process. Once the upload is complete, our servers will test the certificate for validity and report back the test results. If the certificate is valid, the converted certificate will be inserted into the "My SSL Cert" and "My SSL Key" fields. If there are any problems with the certificate, you will be informed once the testing has completed.

Once you have filled out the form for requesting a new site correctly, click the "Request New Site" button to send the request to DOSarrest.

Individual Site Management

Under "Site Management" in the left menu, a list of your VIPs is provided. To manage the settings for a site, click on the VIP you want to manage. A mouse over tooltip will let you know what domain a VIP is handling.
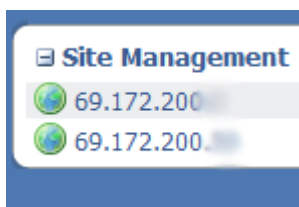
Once you have clicked on a VIP, the management options will be presented. If you would like to disable the site for any reason, you can remove the checkmark from the "Enable Site" checkbox.

The process for managing a site is similar to requesting a new site, but with some differences. When managing a site you have more settings available. The time period for how frequent our servers update the cache for your sites can also be set here.

The basic management options of the site are the same options presented when requesting a new site with some added security options. Only one security option can be enabled at a time. These options should only be enabled during an attack or during a time of suspected attack. While these options are enabled, they can cause unexpected effects; please test your site thoroughly and read the knowledgebase articles. If testing shows that keeping the preferred security option enabled at all times causes no adverse effects, keeping it enabled at all times will give you a higher level of protection in the event an attack does start up.

When uploading a new SSL certificate by clicking on the "Upload SSL Certificate"/"Upload New SSL Certificate" you will be presented with the same SSL utility discussed in the Site Management section of this user guide.

Once the certificate has been properly tested and put into the "My SSL Cert" and "My SSL Key" text areas, you will need to click the "Save Changes" button in order to have the changes applied to your configuration.

Any changes made to the site settings will need to be saved by clicking the "Save Changes" button at the bottom. Once the changes have been saved, DOSarrest will be informed, the changes will be reviewed, and then they will be applied. Once the changes have been applied, an email will be sent to you informing you the updates have been completed.

Security Bypasses

For each site you can manage a list of security bypasses. Security bypasses are used to prevent particular networks from hitting the security mechanisms. For instance, you can add a bypass for the network addresses associated with your company firewall to make sure that staff members behind the firewall will never see the security mechanisms.

To access the management of bypasses, click on the "Manage Bypasses" button at the bottom of the page for the individual site you are configuring.

This will open up the following popup which initially displays a list of bypasses.
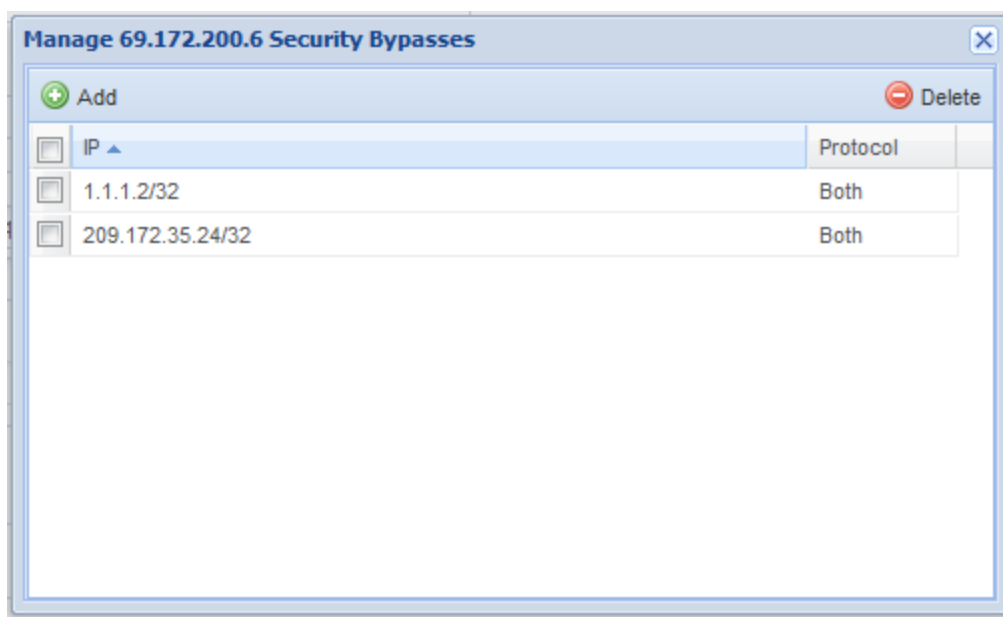
IP security bypasses will whitelist IPs from ever seeing our proxy level security. Once you click on a row and select it, you can click the "Delete" button to delete the bypass. To edit the IP field, click on it, and edit the text directly. It will be saved immediately after you press enter. You can also change the protocol of the entry by clicking it and selecting "HTTP", "HTTPS", or "Both" from the dropdown.

Every time a bypass is newly added, modified, or deleted, DOSarrest is notified of the changes. DOSarrest will then review the changes and apply them. Once the changes have been applied, an email will be sent to you informing you the updates have been completed.

Purging Cache For Individual URLs

To purge or clear the cache for certain URLs, click on the "Purge Cache" button at the bottom of the page for the individual site you are configuring.

A new window will appear, allowing you to enter certain URLs to purge the cache of. They will be relative links, like "/", "/index.html", or "/images/pic5.jpg". Within the textbox, enter the URLs you want to purge the cache of separated by a new line (press enter for a new line), and click "Purge".
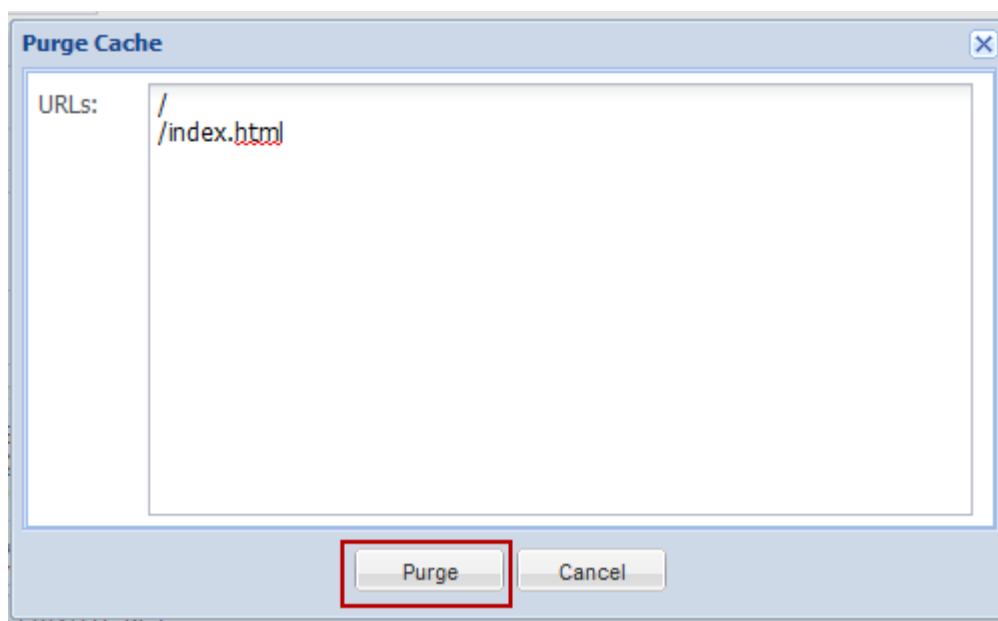
A new window will appear with a list of our servers, and will show you the status of your request.
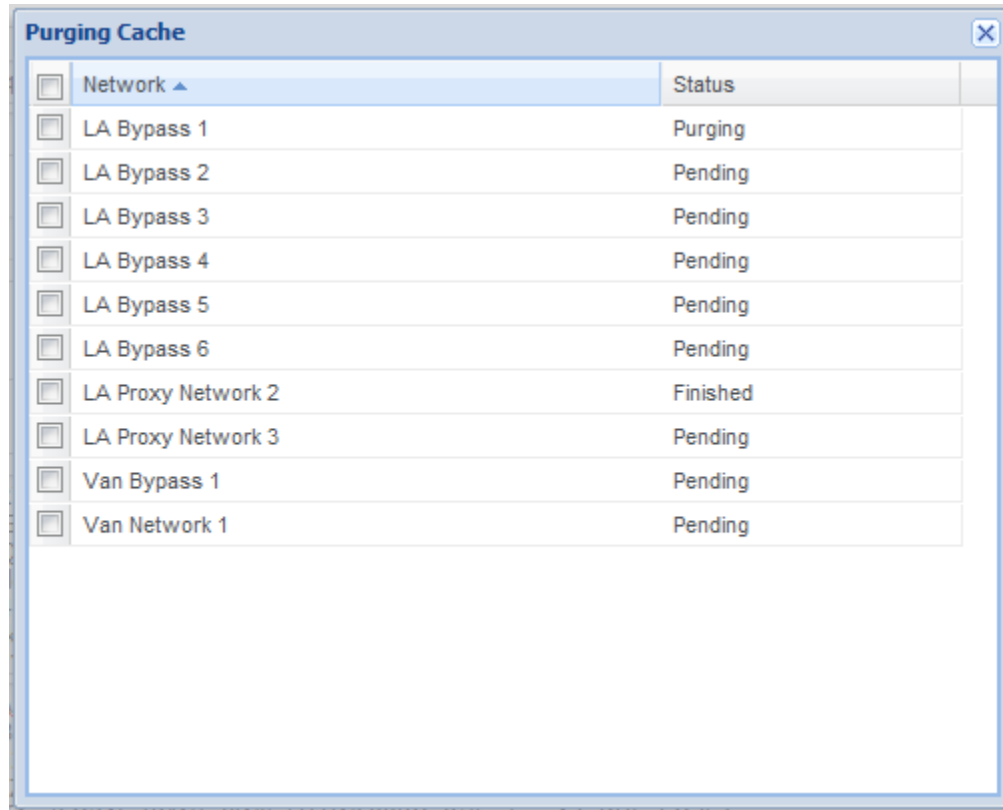
Once the update has been completed, a new popup will appear informing you that the cache for the URLs specified has been purged.
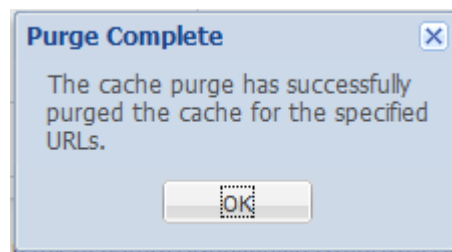
URIs

Within each site, you can also have unique settings for specific URIs. URIs are anything that a user requests from the HTTP server, and are quite flexible to use and manage. For example, you could create a URI that encompasses all files that have specific file extension(s), or a URI that represents all files or addresses that start with a specific string. URIs can also be exact and precise, and can point to just one file or address for your site.

Through using URIs, you can manage your site with a high level of customization and flexibility. For each URI, you can have specific settings like enable or disable caching for that URI only, or enable or disable security mechanisms for that URI. There are also other advanced options available as well, and using URIs can help optimize or protect any type of site. One useful method of using URIs is having caching turned off for your whole site if a large portion of the site is dynamic and cannot be cached, but also configure this URI to cache specific URIs (images, specific folders, etc.) that stay mostly static and can be cached.

You can also use URIs to disable caching content for particular pages or folders. This is necessary for dynamic content that will not function properly when cached. For example, if you have chosen to enable caching for your site, but you have a shopping cart page which you do not want cached, you can turn off caching for the shopping cart page's URI(s), like "cart.php", etc.

Also, if you have a directory of images used to serve banners, you will need to disable our security mechanisms for the URI of that directory. This will prevent our servers from overriding the requests for the banner files with.

To start adding URIs for your site, click on the "Manage URIs" button at the bottom of the page for the individual site you are configuring.

A new window showing the current list of URIs will appear. You can choose to enable/disable Caching and other advanced options for each URI (more explained later).To add a new URI, click on the "Add" button at the top left part of the new window. You can also select an existing URI and click the "Delete" button on the top right part of the window to delete it.
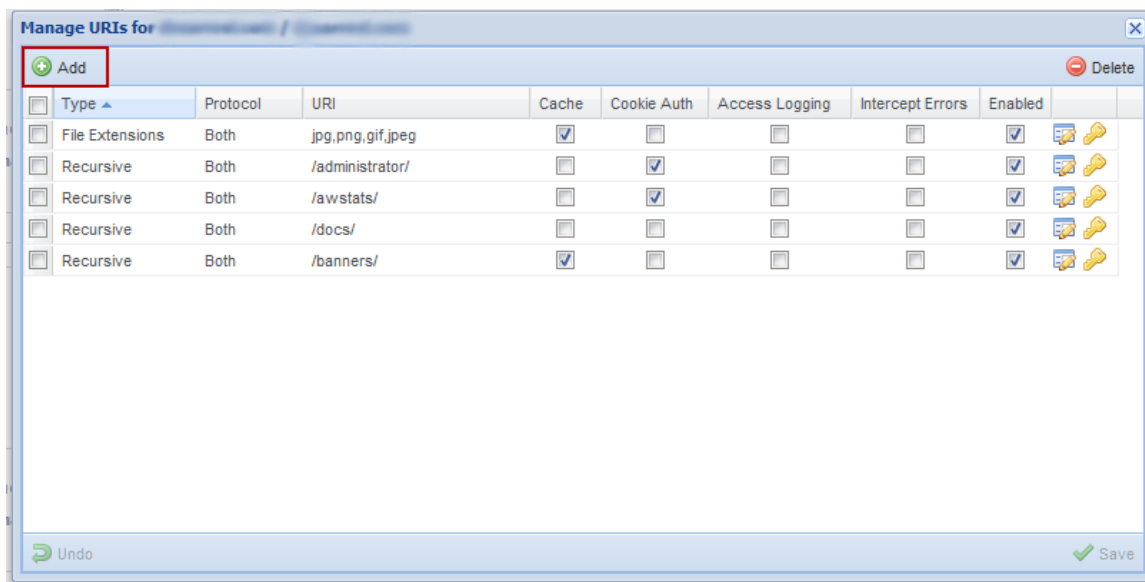
When adding a new URI, there are four types of URIs you can choose from: Recursive, Exact, Exclusive, and File Extensions. Select the drop down next to "Type" to choose one of the options. For protocol, you can choose whether this URI setting applies to HTTP, HTTPS, or both.
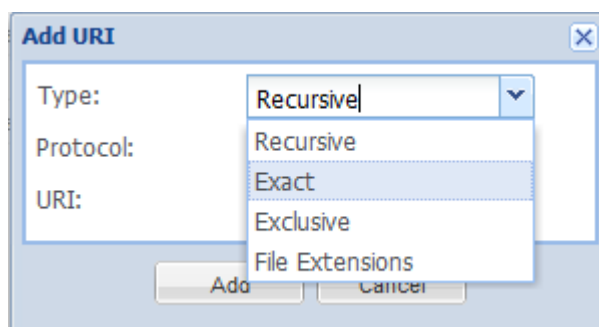
Recursive URIs are wildcard entries, which translates to any addresses that begin with the text specified. For example, entering "/admin/" as the text entry for a Recursive URI can refer to any address a user requests that begins with "/admin/", including "/admin/index.php", "/admin/panel/access.html", "/admin/update.php?page=1" etc. This is particularly useful if you have an admin panel within the folder /admin/, and do not want anything in the admin panel cached. Please note that URIs cannot contain parameters, such as the "?page=1" portion in the last example, so add the URI without the parameters.

However, for Recursive URIs, if any other URI is matched, such as a file extension URI or another Recursive URI with a deeper URI location, then the other URI will be applied. For example, if the address requested was "/admin/picture.jpg", and there were two URI entries, "/admin/" and a File Extension URI entry "jpg,png,gif,jpeg" (File Extension URIs explained later), then the File Extension URI settings will be applied instead of the Recursive one.

Exact URIs are entries that specify exactly what to apply the URI settings to. For example, entering "/cart.php" as the text entry for an Exact URI will apply the URI settings to the file "/cart.php" and only

"/cart.php". This is useful in instances such as when you want to override the global cache setting, and disable caching for just the file "cart.php". However, note that requests like "/cart.php?entry=1" or any addresses that have additional parameters after "/cart.php" would still remain cached, so only choose this setting if the file does not take any parameters. For URIs that use parameters, use Recursive URIs instead.

Exclusive URIs are also wildcard entries like Recursive URIs, and apply to any addresses requested that begin with the text specified. However, unlike Recursive URIs, they take precedence over other URI types, like File Extension URIs. Therefore, if an Exclusive URI is matched, then the settings for that URI will be applied right away, and the system will not check whether other URIs match.
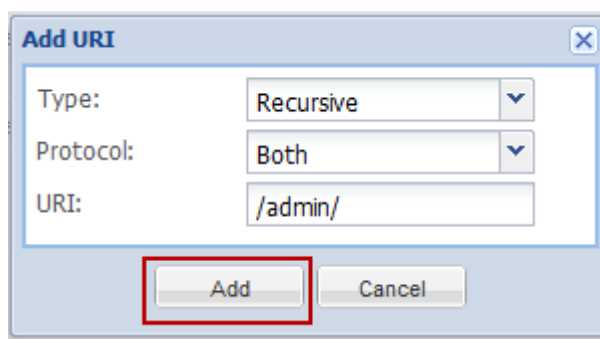
File Extension URIs are any requests for files with the specified file extensions. For example, the entry "jpg,png,gif,jpeg" would specify most image file types, and encompasses requests such as "/images/pic1.jpg", "/icon.gif", or "/layout/img/button.png". Utilizing this type of URI is useful for websites that have completely dynamic content, where all pages have new or specific content every time they are accessed by different users, but the images are relatively static. By enabling the cache setting for the images only, the whole site will still remain dynamic, but all the images on the site will be cached, and therefore site performance would increase greatly. Please note that when entering the extensions, separate multiple extensions with a comma with NO spaces, and do not include the "." before the extension.

Once you have chosen the type of URI select the protocol (HTTP, HTTPS or both) you want to apply it to, and then enter the URI. Click the "Add" button to add the URI.

To manage or edit the different options for the URIs, simply check the option to enable it, or uncheck it to disable it. For example, having a checkmark under the column "Cache" will always ENABLE caching for that URI, and leaving it unchecked will always DISABLE it for that URI. These settings override any global caching or other settings the site has been set to. The option "Access Logging" will enable logging for the specified URI, which will go into the "Logs" area of the DSS. The option "Intercept Errors" will allow the DOSarrest servers to handle error messages (404, 501, etc.) for that URI, instead of using the origin server's error messages. Enabling this can potentially take some load off of the origin server, but will not display any custom error messages your site may have.

You can also edit the URI directly here, by selecting the field. When selecting the field under "Type" or "Protocol", a dropdown will appear where you can change the setting. To edit the "URI" field, click on

the field and it will automatically be editable. Finally, to enable this URI, make sure the checkbox under the "Enabled" column is checked. Save all your settings by clicking the "Save" button on the bottom right.

For some advanced options on the URIs, click on the "Options" on the right side of the URI settings window.
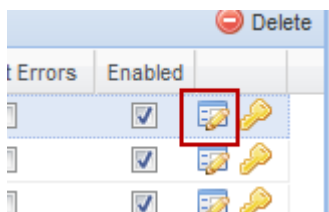
A new window will appear for editing the advanced options of this URI. The "Enable Caching" checkbox is synced with the one in the table; it is also placed here for easy access. Here you can also set the Cache Time, Read Timeout, and Send Timeout. For very large pages or pages that take a long time to process, they may time out before they finish loading. You can override the default setting of 3 minutes for "Read Timeout" in this case, and set a longer timeout period to account for the loading time. Once you are finished with editing the advanced options, click "Change" and the settings will be applied for the URI.
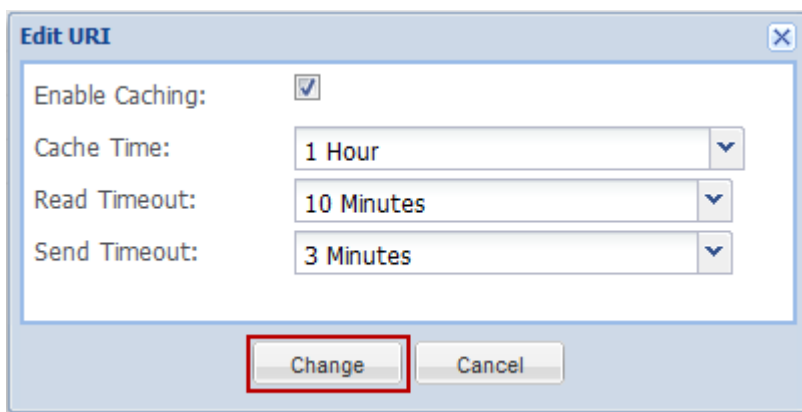

Another advanced option for each URI is available, which is Access Control. To change settings for Access Control, click on the button on the right side of each URI entry.
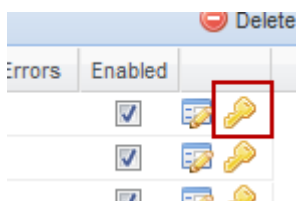

Access Control allows you to set who can or cannot access certain URIs. For example, you may want to restrict the admin section of the site to certain IPs. You can set those permissions in this area by

adding the admin IPs as "Allow" entries at the top, and then set an entry for "all" as a "Deny" entry at the bottom to deny all other IPs.
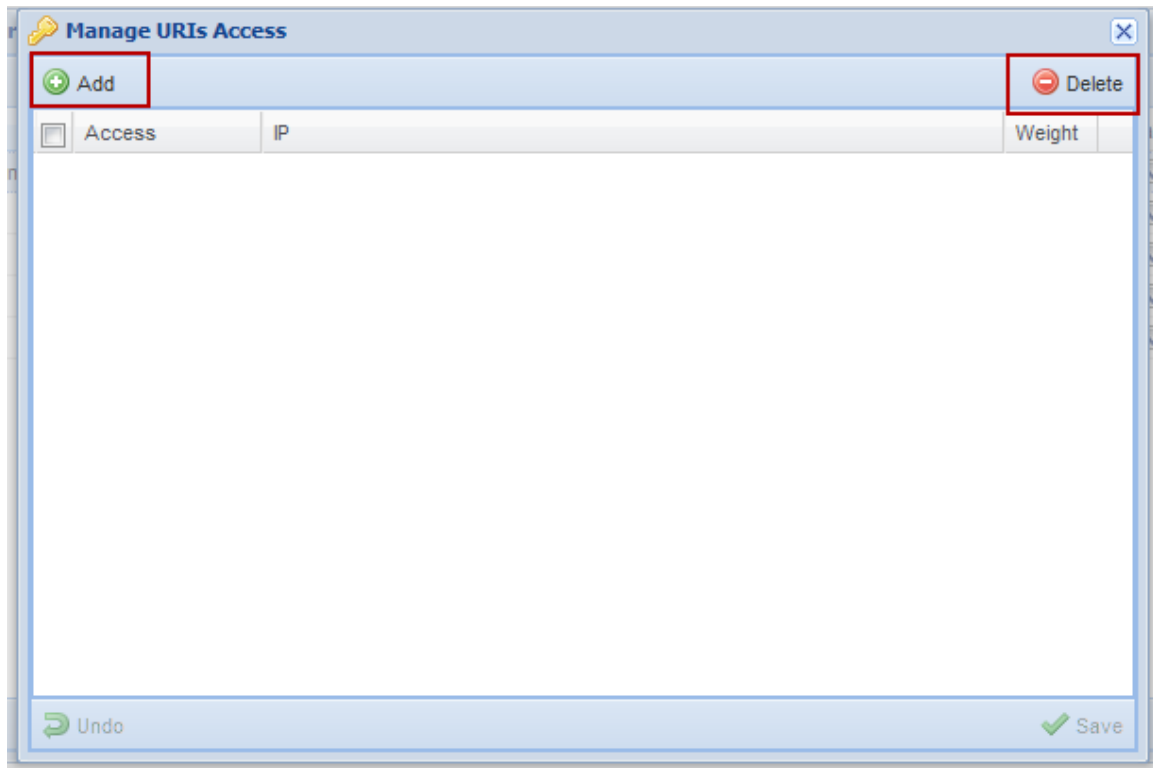
Click on the "Add" button on the top left corner to add an IP to allow/deny. To delete an IP, select the entry, and click on the "Delete" button on the top right corner. When clicking "Add", a new popup window will appear.
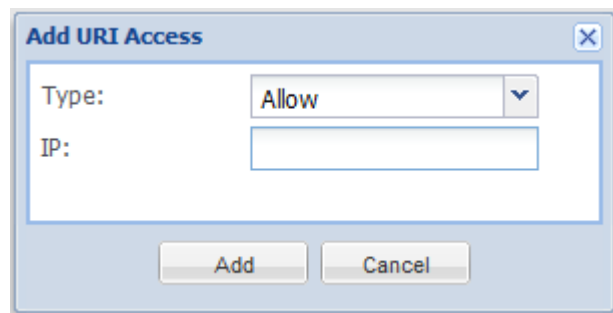
Under "Type", you can choose to either Allow (whitelist) or Deny (blacklist) the IP. Then, enter the IP into the textbox, and click "Add" to add this entry. Please note that you can enter a normal IP, a CIDR entry, or "all".
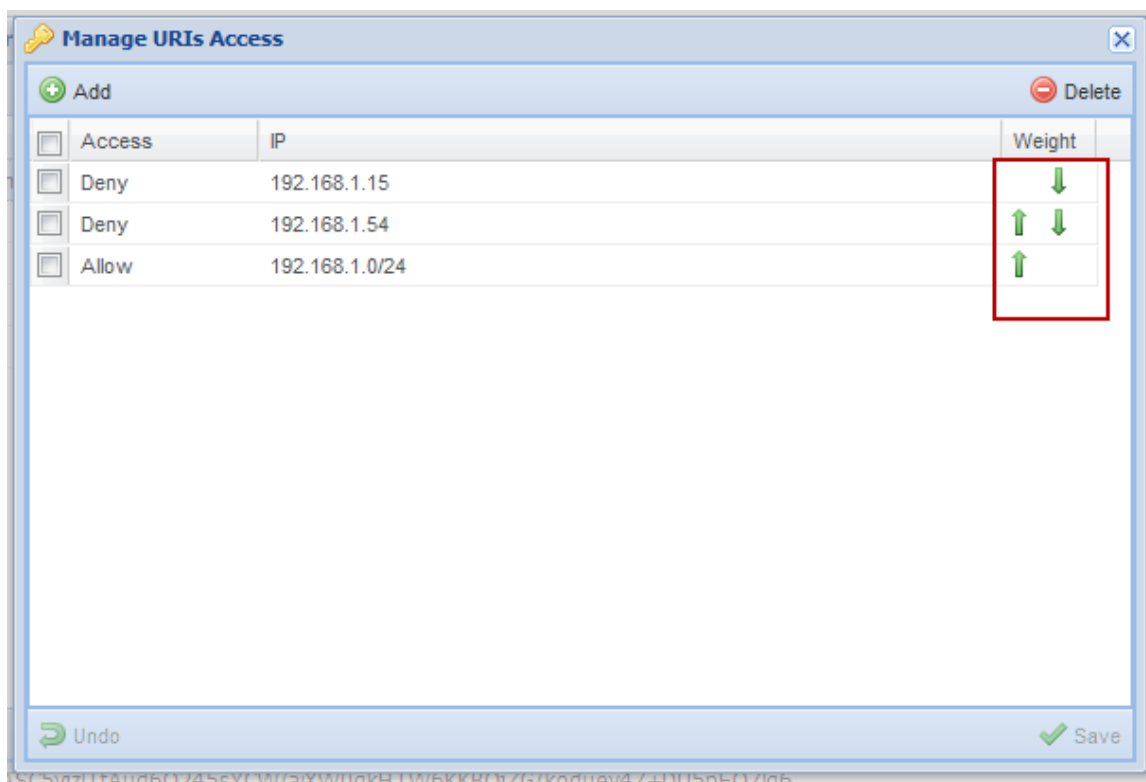
After adding several entries, you can change the order of when they are applied in the "Weight" column. Click on the arrow pointing towards the top to move an entry upwards, and click on the arrow pointing towards the bottom to move an entry downwards.

The order of the entries is very important, as the system will apply the deny/allow setting to whichever entry it matches first. In the above example, 192.168.1.15 will be denied right away, even though it is within the subnet 192.168.1.0/24, since it is the first entry. The same applies for the second entry, 192.168.1.54. However, all other entries within the 192.168.1.0/24 subnet will be allowed, even if there are deny entries for them below this entry (there are none in this example).

Also, within this window, you can make changes to any of the fields by clicking on them. A dropdown menu will appear for "Access", and you can type directly into the field for "IP". Click "Save" on the bottom right of the window to save the changes afterwards.